nafn.gov.uk
Data & Intelligence Services

Intelligence Management

3 x 5 x 2

Aims and Objectives

- What is intelligence?
- The Intelligence Report
- Content
- Classification (3x5x2)
    - Source Evaluation
    - Intelligence Evaluation
    - Dissemination
- Do's and Don'ts
- Intelligence Confidence Matrix

What is intelligence?

- Information that has undergone an evaluation process to assess its worth
- Intelligence is graded by using the 3x5x2 aspect of the National Intelligence Model
- The use of the 3x5x2 grading system should mean uniformity to all pieces of intelligence
- Any staff member should be able to judge the intelligence and act on it accordingly simply by using the 3x5x2 grading system

Intelligence Report

- **An Intelligence Report is used to:**
  - **Submit and Evaluate Information, and**
  - **Manage Dissemination of Intelligence**
- **It protects the source and contributes to an audit trail of the intelligence.**
- **Standardisation of reporting provides a shared confidence between law enforcement communities and partner agencies**

Information Content

The information content should comply with the basic principles of what, when, where, why, who and how.

Information should be clear, concise and without abbreviations. The information must be of value and understood without the need to refer to other information sources.

The body of the report should give no indication of the nature of the Source, whether human or technical, or the proximity of the Source to the information.

Where possible, the information should be corroborated and its provenance established.

Classification

All reports should be allocated an appropriate classification. The majority of information/intelligence that the law enforcement agency holds contains personal or sensitive data.

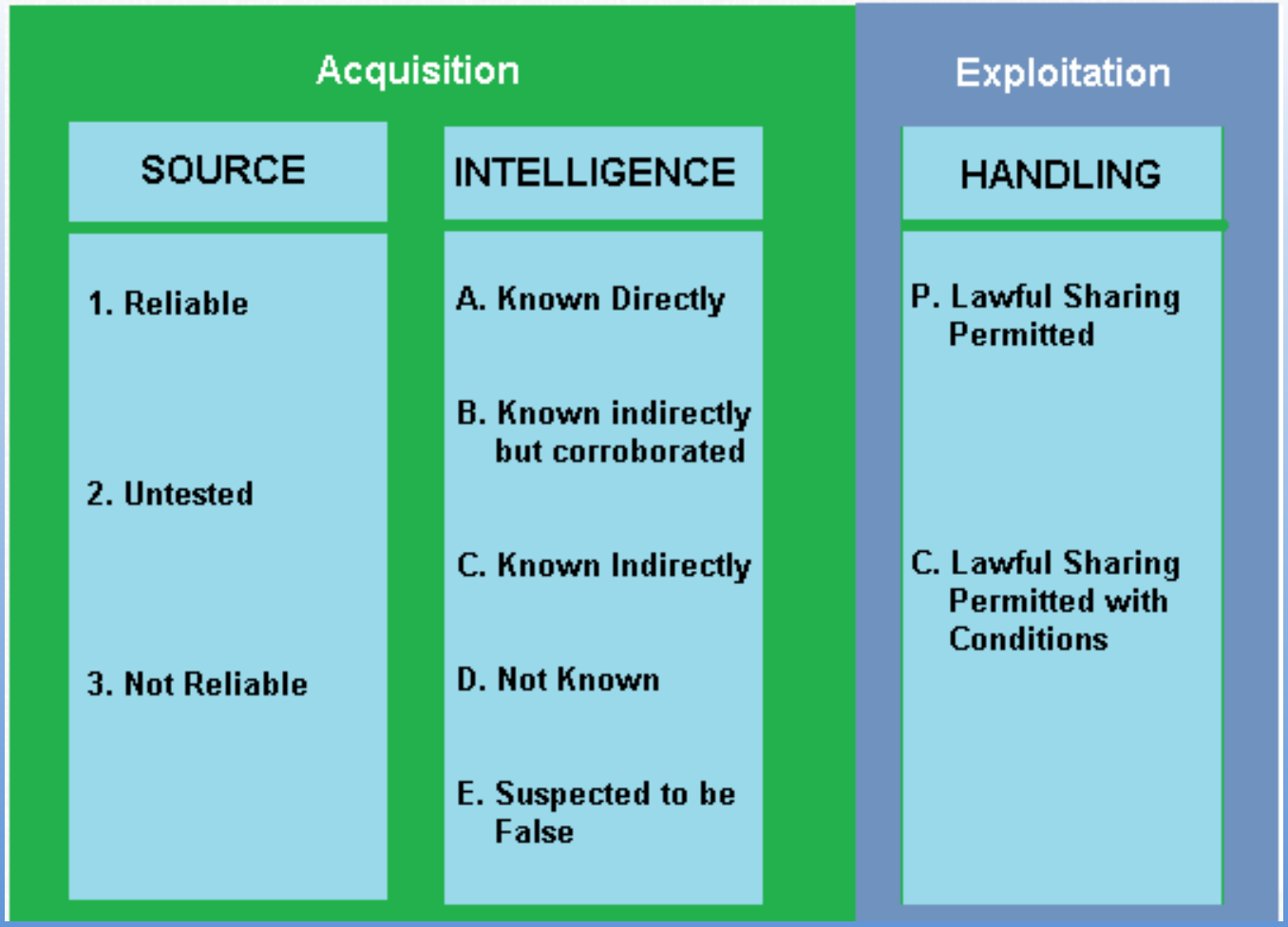
It is important that the classification reflects the level of sensitivity and degree of protection required by the report.

Duty of Care

The ownership of the risk to the Source always remains within the originating organisation. When intelligence is disseminated outside the originating organisation, any handling conditions must be adhered to by the receiving organisation. When this doesn't happen, both organisations may be held accountable for any consequences.

nafn.gov.uk
Data & Intelligence Services

Gradings



Source Evaluation

The Source of the information can be either the name and address of the person providing the information or an Intelligence Source Reference number.

In order to avoid any chance of compromise, the details of the person providing the information should not be placed in the main body of the report.

The final report should not detail the true identity of any Source, either within a source field or the main body of the text; this includes law enforcement officers and staff as information sources.

Organisations must have measures in place to ensure that the correct identity of the Source is not revealed.

Source Evaluation

1 = Reliable

This grading is used when the source is believed to be both competent and information received is generally reliable.

This may include information from human intelligence, technical, scientific and forensic sources.

It is important that the two tests of competence and veracity of past intelligence are both met before a source is considered to be reliable.

Where either test is not met, Not Reliable should be selected and the ground to doubt the reliability is specified.

Examples – Technical products e.g. DNA, fingerprints, CCTV

Source Evaluation

2 = Untested

This relates to a source that has not previously provided information to the person receiving it or has provided information that has not been substantiated.

The source may not necessarily be unreliable, but the information provided should be treated with caution.

Before acting on this information, corroboration should be considered.

This would apply to information when the source cannot be determined, for example, members of the public, Crimestoppers.

Source Evaluation

3 = Not Reliable

This should be used where there are reasonable grounds to doubt the reliability of the Source.

These should be specified within the Intelligence Report risk assessment and may include concerns regarding the authenticity, trustworthiness, competence or motive of the Source or confidence in the technical equipment.

Corroboration should be sought before acting on this information.

Examples – members of the public with a potentially malicious motive, individual with a history of making false allegations

Intelligence Evaluation

A = Known Directly to the Source

Refers to information obtained first-hand, e.g. through witnessing of the event or refers to live evidence.

Care must be taken to differentiate between what a Source witnessed themselves and what a Source has been told or heard from a third party.

Intelligence Evaluation

B = Known Indirectly to the Source but Corroborated

Refers to information that the Source has not witnessed themselves, but the reliability of the information can be verified by separate information that carries the information/intelligence of assessment of A.

This corroboration could come from technical sources, other intelligence, investigations or enquiries.

Care should be taken when ascertaining corroboration to ensure that the information that is presented as corroboration is independent and not from the same original Source.

Intelligence Evaluation

C = Known Indirectly to the Source

Applies to information that the Source has been told by someone else. The Source does not have first-hand knowledge of the information as they did not witness it themselves.

Intelligence Evaluation

D = Not Known

Applies where there is no means of assessing the information.

This may include information from an anonymous Source, or partners such as Crimestoppers.

Intelligence Evaluation

E = Suspected to be False

Treat with extreme caution

Regardless of how the Source came upon this information, there is a reason to believe the information provided is false.

If this is the case, the rationale for why it is believed to be false should be documented in the Intelligence Report.

Examples – malicious/non-malicious callers, CHIS engaging in criminal activity and providing information to deflect attention from themselves, or to prepare a defence of working for the police should they be arrested.

Dissemination

Handling Codes and Conditions

Handling codes are a control mechanism for intelligence sharing.

The risks associated with sharing intelligence must always be weighed against the potentially greater risk of not sharing.

Handling codes are supported by conditions for intelligence sharing.

Before disseminating intelligence, the person disseminating should ensure they are familiar with the appropriate legislation and their organisation's policies, standard operating procedures and other frameworks.

Dissemination (P1)

P = Lawful Sharing Permitted

In order to share this intelligence there must be:

- **a legitimate purpose**
- **local protocols in place**
- **a legitimate need to receive it.**

Lawful legitimate purposes can be defined as to:

- **assist others to protect life or property**
- **assist to preserve order**
- **prevent the commission of offences**
- **assist others to bring offenders to justice**
- **linked to any duty or responsibility arising from common or statute law.**

Dissemination (P2)

P = Lawful Sharing Permitted

Lawful sharing includes other government departments, private and voluntary sectors.

Specific questions need to be asked when considering dissemination of Code P intelligence. For example:

- **are there legal obligations?**
- **who is asking for it?**
- **why do they want it?**
- **what are they going to do with it?**

Dissemination to European Economic Area (EEA) law enforcement agencies is permitted.

Dissemination (P3)

P = Lawful Sharing Permitted

If there are concerns around how widely the intelligence may be disseminated, Code C applies. It may not be appropriate to disseminate all of the intelligence and the merits of redaction should be considered.

Dissemination to (non-EEA) foreign law enforcement agencies should be risk assessed on an individual basis. The Data Protection Act 2018 allows for personal information to be disseminated outside the EU only after the risks have been assessed and on the grounds of substantial public interest. Public interest in this context includes tackling serious crime and the maintenance of the security and integrity of law enforcement agencies.

EXTREME CARE should be taken when handling intelligence received from HMRC as further unauthorised dissemination may result in the commission of a criminal offence.

Dissemination (C)

C = Lawful Sharing Permitted with Conditions

This code permits dissemination but requires the receiving agency to observe conditions as specified. Application of this code means the originator has applied specific handling instructions in respect of this information.

An application for public interest immunity should be considered if the intelligence is subsequently used in court.

Handling conditions should be contained within the appropriate section of the Intelligence Report.

The recipient must abide by the handling conditions. The originator must be contacted by the recipient before they conduct any further activities outside the conditions.

Do's and Don'ts

Do

- Insert the contact and provenance details – ALWAYS
- Use multiple grading within a single piece in intelligence, if necessary
- Double check the grading

Don't

- Ever mention the name or any details of the informant, or how they came across the information
- Use unnecessary wording, i.e. "Information received that…" or "whilst out on a job I came across…"
- Use puns, opinions or sarcasm in an entry – however tempting it is!

Intelligence Matrix

The following matrix provides an indication of the level of confidence that can be taken in the intelligence dissemination.

This informs decision-making and supports interoperability between agencies/organisations.